KINGDOM OF MOROCCO

NATIONAL DEFENSE ADMINISTRATION

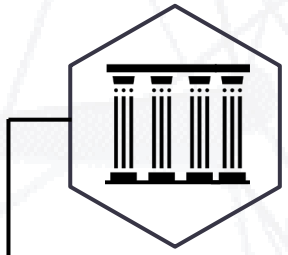
THE NATIONAL CYBERSECURITY STRATEGY 2030

GENERAL DIRECTORATE OF INFORMATION SYSTEMS SECURITY

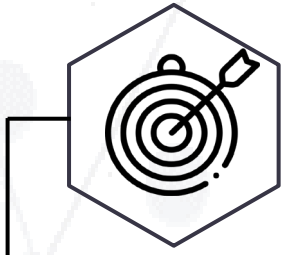
Vision

For a reliable , secure and resilient national cyberspace supporting Kingdom's digital transformation, promoting economic prosperity and ensuring citizens' well-being

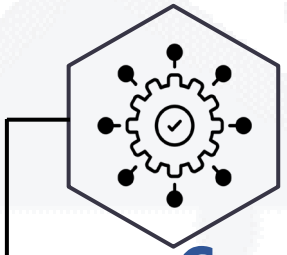
Strategy in numbers



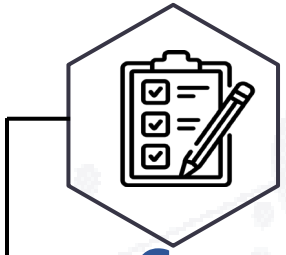
04
Pillars



11
Strategic objectives



26
Initiatives



60
Actions

Pillar 1 : National cybersecurity governance - Institutional and legal framework

Maintain and strengthen the legal and normative framework

- Periodically review and strengthen the national cybersecurity legal and normative framework
- Carry out the sectoral adaptation of the legal and normative framework

Improve national coordination mechanisms

- Improve coordination and information sharing between stakeholders in the protection of CIs
- Improve coordination between law enforcement and cyber intelligence agencies
- Promote and develop coordination mechanisms with private actors

Pillar 2 : Security and resilience of national cyberspace

Support decision-making by data-driven policies

- Establish an overview of the national cybersecurity landscape
- Establish mechanisms for collecting data, metrics and indicators on national cybersecurity capabilities

Promote the implementation of cybersecurity standards and norms

- Strengthen the existing offer by implementing new qualification and labeling schemes for cybersecurity products, services or providers
- Establish national cybersecurity certification schemes for public and private organizations

Strengthen national capacities for prevention, management and response to cyber incidents and crises

- Strengthening national readiness and responsiveness to address cyber crises
- Develop sectoral capabilities in cyber incident management

Consolidate resilience of critical infrastructure information systems

- Maintain an updated mapping of CIs and their sensitive information systems and clarify cross-sector dependencies
- Strengthen audit and control activities to verify CIs compliance
- Enhance the resilience of telecom operators and digital service operators

Pillar 3 : Capacity building and awareness

Develop a cybersecurity culture within the society

- Raise citizens' awareness about threats and security risks inherent in cyberspace
- Implement awareness campaigns for public and private sectors
- Introduce cybersecurity awareness modules at school level

Strengthen human resources capacities in cybersecurity

- Upgrade and enhance cybersecurity training programs in universities and professional training centers
- Promote professional certification to build a pool of certified cybersecurity experts
- Improve multidisciplinary continuous training offers for cybersecurity managers
- Adapt the cybersecurity training offer to business needs

Support the development of the national cybersecurity ecosystem and encourage innovation

- Encourage development of cybersecurity ecosystem at national level
- Support research and development within universities and training centers

Pillar 4 : Regional and international cooperation

Strengthen and promote active participation at regional and international level on cybersecurity issues

- Actively participate in international forums and processes
- Support and strengthen Kingdom's positioning in cybersecurity at regional and international levels

Development of bilateral cooperation

- Increase bilateral cooperation with countries in the areas of information sharing and capacity building